최종안 – 2006 년 8 월 29 일

반테러 세관 - 무역 파트너십(C-TPAT)
보안 기준
외국 제조업체

본 최저 보안 기준은, 근본적으로 테러범과 테러의 도구를 세계 공급망으로 도입시킬 수 있는 분실, 도난 및 밀수의 위험을 완화시키는 공급망 성능의 최적화를 위해 마련된 효과적인 보안 방법을 외국 제조업체가 마련하는 기초 요소의 역할을 합니다. 내부의 음모를 통하여 세계 상업을 대상으로 하는 범죄 요소들의 결정 및 범위는 회사 특히 외국 제조업체가 자체의 보안 방식을 강화시키는 것을 요구합니다.

최소한 일년에 한 번 혹은 고조된 위험, 보안 위반 또는 사건과 같은 상황이 요구하는 바에 따라, 외국 제조업체는 반드시 다음의 C-TPAT 보안 기준에 근거하여 자사의 공급망에 대한 종합 평가를 수행해야 합니다. 외국 제조업체가 다른 외국 시설이나 창고 또는 기타 요소 등에게 자신의 공급망의 요소를 아웃소싱하거나 하청하는 경우, 해당 외국 제조업체는 그러한 사업 파트너와 반드시 협력하여, 적절한 보안 대책이 수립되고 공급망 전반에 걸쳐 준수되도록 해야 합니다. C-TPAT 목적 상의 공급망은 현장(제조재/공급재/판매자)으로부터 분배 지점으로 정의되며, C-TPAT 구성원들이 사용하는 다양한 사업 모델들을 인식합니다.

C-TPAT 는 국제 공급망 및 보안 방식의 복잡성을 인식하며, 위험에 근거하는 보안 대책의 적용 및 구현을 인정합니다.[1] *그러므로 이 프로그램은 구성원의 사업 모델에 근거하는 보안 계획의 유연성과 맞춤화를 허용합니다.*

이 문서 전체에 나와 있는 적절한 보안 대책들을 위험에 근거하여 외국 제조업체의 공급망 전반에 구현시키고 유지해야 합니다.[2]

<u>사업 파트너 요구조건</u>
외국 제조업체는 운송업체, 기타 제조업체, 제품 공급업체 및 납품업체(부품과 원료 공급업체 등)를 포함하는 사업 파트너의 선택에 필요한 검증 가능한 프로세스를 서면으로 가지고 있어야 합니다.

- 보안 절차
  C-TPAT 인증에 대한 자격이 있는 사업 파트너(운송업체, 수입업체, 항구, 터미널, 중개인, 병합자 등)에 대하여는, 외국 제조업체는 이러한 사업 파트너가 C-TPAT 인증을 받았는지 여부를 표시하는 문서(예: C-TPAT 증명서, SVI 번호 등)를 소지해야 합니다.

  C-TPAT 인증에 대한 자격이 없는 사업 파트너에 대하여는, 외국 제조업체는 사업 파트너에게 서면/컴퓨터 확인을 통하여 C-TPAT 보안 기준에 부합함을 보이도록 요구해야 합니다(예: 계약적 의무; 사업 파트너의 중역에 의한 준수를 증명하는 서신; C-TPAT 보안 기준 혹은 이에 상응하는 외국 세관 기관이 집행하는 세계세관기구(WCO)의 인증을 받은 보안 프로그램에 대한 준수를 보여주는 사업 파트너의 진술서; 혹은 외국 제조업체의 보안

---

[1] 외국 제조업체는 사업 모델에 근거하여 공급망 전체에 걸쳐 위험을 결정하는 문서화되고 승인가능한 프로세스를 마련해야 합니다(예: 물량, 국적, 라우팅, C-TPAT 회원, 공개 출처 정보를 통한 테러범의 위협 가능성, 미흡한 보안, 과거 보안 사건 등).
[2]외국 제조업체는 사업 모델에 근거하여 공급망 전체에 걸쳐 위험을 결정하는 문서화되고 승인가능한 프로세스를 마련해야 합니다(예: 물량, 국적, 라우팅, 공개 출처 정보를 통한 테러범의 위협 가능성 등)

설문조사 완료 및 제공). 문서화된 위험 평가 과정에 근거하여, C-TPAT 자격이 없는 사업 파트너는 외국 제조업체에 의한 C-TPAT 보안 기준의 준수 확인을 받아야 합니다.

- **현장**
  외국 제조업체는 사업 파트너가 현장에서의 출하, 조립 또는 제조의 무결함 강화를 위하여 C-TPAT 보안 기준에 일치하는 보안 과정 및 절차를 개발하도록 해야 합니다. 사업 파트너의 공정 및 시설들의 규칙적인 검토는 위험에 근거하여 실행해야 하며, 외국 제조업체가 요구하는 보안 표준을 유지해야 합니다.

- **세관의 공급망 보안 프로그램의 참가/인증**
  세관이 집행하는 공급망 보안 프로그램의 인증을 취득한 현재나 장래의 사업 파트너는 외국 제조업체에게 그 참가 상태가 보이도록 해야 합니다.

- **보안 절차**
  미국향 선적에 대해, 외국 제조업체는 운송 서비스를 다른 운송업체에게 하청 주는 C-TPAT 운송업체가, 다른 C-TPAT 승인을 받는 운송업체나 사업 파트너 요구조건에 요약되어 있는 C-TPAT 보안 기준을 부합하는 비 C-TPAT 운송업체를 사용하는지 감지해야 합니다.

  외국 제조업체는 트레일러와 컨테이너의 선적에 대한 책임이 있으므로, 운송업체와 협력하여 효과적인 보안 절차 및 통제 기능이 선적 지점에서 구현되도록 재보장해야 합니다.

<u>**컨테이너 및 트레일러 보안**</u>

컨테이너 및 트레일러에 대한 무결성을 유지하여 자재 및/또는 사람의 무단 도입으로부터 보호해야 합니다. 선적 지점에는 선적 컨테이너와 트레일러의 무결성을 적절히 밀봉하고 유지하는 절차가 있어야 합니다. 최고 보안 인증을 미국향의 모든 선적된 컨테이너와 트레일러에 붙여야 합니다. 모든 봉인은 최고 보안 인증에 해당하는 기존의 PAS ISO 17712 표준을 부합 또는 초과해야 합니다.

위험 평가를 위하여 컨테이너나 트레일러에게 사람의 은폐나 밀수를 점검하는 지역에 있어서, 그 절차는 제조 시설 혹은 선적 지점에서 이러한 위험을 해결할 수 있도록 준비되어야 합니다.

- **컨테이너 검사**
  선적 전에 컨테이너 구조의 물리적 무결성을 확인하며 도어 잠금 장치의 신뢰성이 포함되는 절차를 마련해야 합니다. 모든 컨테이너에 대하여 일곱 가지 검사 과정이 권장됩니다:
  - 정면 벽
  - 왼쪽 측면
  - 오른쪽 측면
  - 바닥
  - 천정/지붕
  - 옥내외 도어
  - 외부/차대

- **트레일러 검사**
  선적 전에 트레일러 구조의 물리적 무결성을 확인하며 도어 잠금 장치의 신뢰성이 포함되는 절차를 마련해야 합니다. 모든 트레일러에 대해 다음 검사 과정이 권장됩니다:

- 제 5 륜 부위 - 내추럴 콤파트먼트/스키드 플레이트 점검
- 외부 - 정면/측면
- 뒤면 - 범퍼/도어
- 정면 벽
- 좌측
- 우측
- 마루
- 천정/지붕
- 도어 내외부
- 외부/차대

- **컨테이너 및 트레일러 봉인**
  연속적인 봉인의 무결성을 포함하여 트레일러와 컨테이너의 밀봉은 안전이 확보된 공급망의 주요 요소이며, 외국 제조업체의 C-TPAT 에 대한 약정의 중대한 일부입니다. 외국 제조업체는 최고 보안 인증을 미국향의 모든 선적된 컨테이너와 트레일러에 붙여야 합니다. 모든 봉인은 최고 보안 인증에 해당하는 기존의 PAS ISO 17712 표준을 부합 또는 초과해야 합니다.

  서면 절차는 선적된 컨테이너나 트레일러에 봉인을 어떻게 통제하고 첨부하는지 규정해야 하며, 손상된 봉인 및/또는 컨테이너/트레일러를 파악하여 미국 세관 및 국경 보호대 또는 적절한 외국 기관에 보고하는 절차를 포함해야 합니다. 지정된 직원만이 무결성 목적을 위한 봉인을 배포해야 합니다.

- **컨테이너 및 트레일러 보관**
  외국 제조업체의 통제 하에 있거나 외국 제조업체의 시설 내에 위치한 컨테이너 및 트레일러는, 무단 출입 및/또는 조작을 방지하기 위해 보안이 확보된 장소에 보관해야 합니다. 컨테이너/트레일러 또는 컨테이너/트레일러 보관 장소로의 무단 출입을 보고하고 무력화하는 절차를 마련해야 합니다.

물리적 출입 통제

출입 통제 기능은 시설에 대한 무단 진입을 방지하며 사원과 방문자의 통제를 유지하고 회사 자산을 보호합니다. 출입 통제 기능에는 모든 출입 지점에서 모든 사원과 방문자 및 납품업체에 대한 신원을 파악하는 것이 포함됩니다.

- **사원**
  신원 파악 및 출입 통제 목적을 위한 사원 신원파악 체계를 마련해야 합니다. 사원의 보안이 요구되는 장소에 대한 출입은 직무 수행상 필요한 경우에만 허용되어야 합니다. 회사 관리자나 보안 담당자는 사원, 방문자 및 납품업체의 신분증 배지에 대한 발급과 취소를 충분히 통제해야 합니다. 출입 통제 장치(예: 열쇠, 키카드 등)의 발급, 제거 및 변경에 대한 절차를 반드시 문서화해야 합니다.

- **방문자**
  방문자는 도착 즉시 문서화 목적을 위해 사진 신분증을 제시해야 합니다. 모든 방문자는 에스코트를 받아야 하며 임시 신분증을 보이도록 착용해야 합니다.

- **배달 (우편 포함)**

모든 납품업체는 도착 즉시 문서화 목적을 위해 적절한 업체 ID 및/또는 사진 신분증을 제시해야 합니다. 도착하는 패키지와 우편은 규칙적인 선별 검사를 거친 후에 배포해야 합니다.

- **무단 출입자에 대한 신분증 요구 및 제거**
  무단 출입자 또는 신원 미확인자에 대한 신원 파악, 신분증 제시 및 해결을 위한 절차를 마련해야 합니다.

<u>인사 보안</u>
장래의 사원을 선별하고 기존 사원을 규칙적으로 점검하는 절차를 마련해야 합니다.

- **채용 전 확인**
  직장 경력과 참조인 등 신청서 정보는 채용 전에 반드시 확인해야 합니다.

- **배경 점검/조사**
  해외 법규와 일치하도록, 장래 사원에 대한 배경 점검 및 조사를 수행해야 합니다. 일단 고용되면, 규칙적인 점검 및 재조사를 원인 및/또는 사원 직책의 민감성을 기준으로 수행해야 합니다.

- **해고 절차**
  회사에서는 해고된 사원에 대한 신분증, 시설 및 시스템의 접근을 취소시키는 절차를 실시해야 합니다.

<u>절차상 보안</u>
공급망에서 화물의 운송, 취급 및 보관과 관련된 프로세스들의 무결성 및 보안을 보장하는 절차를 마련해야 합니다.

- **문서 처리**
  상품/화물의 처리에 사용되는 모든 정보는 명확하고 완벽하며 정확하고 또한 교환, 손실 또는 오류 정보의 개입으로부터 보호되도록 보장하는 절차를 마련해야 합니다. 문서 통제 기능에는 컴퓨터 접속 및 정보의 방호가 포함되어야 합니다.

- **적하목록 절차**
  화물의 무결성 보장을 위하여, 사업 파트너로부터 수령하는 정보가 정확하고 적기에 보고되도록 하는 절차를 마련해야 합니다.

- **선적 및 인수**
  선적되어 출발하는 화물은 화물 적하목록에 있는 정보와 대조하여 일치해야 합니다. 화물은 내용을 정확히 기재해야 하며, 중량, 라벨, 표 및 개수를 표시하고 확인해야 합니다. 출발하는 화물은 구매 또는 배달 주문에 대해 확인해야 합니다. 화물을 배달하거나 인수하는 운전사의 신원을 확인한 다음 화물을 인수하거나 방출해야 합니다. 들어가고 나가는 물품의 적기 이동을 추적하는 절차 또한 확립해야 합니다.

- **화물 불일치**

모든 부족, 노후 및 기타 상당한 불일치 또는 이상한 내용은 반드시 해결하거나 적절히 조사해야 합니다. 이상한 내용, 불법 또는 의심이 가는 활동이 검출되면, 필요에 따라 세관 및/또는 기타 적절한 경찰 기관에 통지해야 합니다.

<u>물리적 보안</u>

해외에 위치한 화물 취급 및 보관 시설에는 무단 출입으로부터 보호하는 물리적 장벽 및 방해물이 있어야 합니다. 외국 제조업체는 해당되는 경우 자신의 공급망 전체에 걸쳐 다음의 C-TPAT 물리적 보안 기준을 포함시켜야 합니다.

- 울타리
  주변 울타리는 화물 취급 및 보관 시설 주위를 둘러싸야 합니다. 화물 취급 구조 내에 위치한 내부 울타리는 국내, 국외, 고가치 및 위험 화물의 격리에 사용해야 합니다. 모든 울타리는 무결성과 손상 여부를 규칙적으로 검사해야 합니다.

- 게이트 및 초소
  차량 및/또는 인원이 출입하는 게이트에는 반드시 인력을 배치하고 감시해야 합니다. 게이트의 숫자는 적절한 출입과 안전에 필요한 만큼 최저로 유지해야 합니다.

- 주차
  개인 차량은 화물 취급 및 보관 장소의 내부나 주위에서의 주차를 금지해야 합니다.

- 건물 구조
  건물은 불법 출입에 견디는 자재로써 건축해야 합니다. 구조물의 무결성은 규칙적 검사와 수리로서 보수유지해야 합니다.

- 잠금 장치 및 열쇠 통제
  모든 외부 및 내부의 창문, 게이트 및 울타리는 잠금 장치로써 보안을 유지해야 합니다. 관리 및 보안 인원은 모든 자물쇠와 열쇠의 발급을 통제해야 합니다.

- 조명
  다음 지역을 포함하여 시설 내외에는 반드시 충분한 조명을 제공해야 합니다: 출입구, 화물 취급 및 보관 지역, 울타리 선, 주차 지역.

- 알람 장치 및 비디오 감시 카메라
  알람 장치 및 비디오 감시 카메라를 활용하여 부지를 감시하고 화물 취급 및 보관 지역에 대한 무단 출입을 방지해야 합니다.

<u>정보 기술 보안</u>

- 암호 보호
  자동화 장치는 규칙적인 암호의 변경을 요구하는 개인적으로 지정된 어카운트를 사용해야 합니다. IT 보안 정책, 절차 및 표준을 반드시 마련해야 하며 교육을 통하여 사원에게 제공해야 합니다.

- **책임**
  부적절한 출입, 부정 조작 또는 사업 데이터의 변조 등 IT 의 남용을 파악하는 시스템을 설치해야 합니다. 모든 시스템의 위반자는 그 남용에 따른 적절한 징계 조처를 받아야 합니다.

<u>보안 교육 및 위협 인지도</u>

보안 인원은 테러범 및 밀수업자가 가하는 위협을 인지하고 그 인식을 고취시키는 위협 인식 프로그램을 공급망의 각 지점에 확립하고 유지해야 합니다. 사원들은 상황과 그 보고 방법을 알리기 위해 마련한 절차에 대해 알아야 합니다. 선적 및 인수 지역 그리고 우편을 수집하고 개봉하는 직원들에게는 추가의 교육을 제공해야 합니다.

그 밖에도 화물의 무결성을 유지, 내부의 음모를 인식 그리고 출입 통제 기능의 보호를 위해 도움이 되는 구체적인 교육을 사원에게 제공해야 합니다. 이러한 프로그램들은 사원의 적극적인 참여를 위한 인센티브를 제공해야 합니다.